From:	Lincoski, John
Sent:	Fri 5/6/05 12:57 PM
Subject:	TRADEMARK APPLICATION NO. 78279935 - CONTENT ALARM - TML

UNITED STATES PATENT AND TRADEMARK OFFICE

SERIAL NO: 78/279935

APPLICANT: Tablus, Inc.

78279935

CORRESPONDENT ADDRESS:
John Alumit
Patel & Alumit, PC
20121 Ventura Blvd., Suite 302
Woodland Hills CA 91364

BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD ON APPEAL

MARK: CONTENT ALARM

CORRESPONDENT'S REFERENCE/DOCKET NO: TML

CORRESPONDENT EMAIL ADDRESS:
jalumit@tmlawoffices.com

Please provide in all correspondence:

1. Filing date, serial number, mark and applicant's name.
2. Date of this Office Action.
3. Examining Attorney's name and Law Office number.
4. Your telephone number and e-mail address.

EXAMINING ATTORNEY'S APPEAL BRIEF

Applicant Tablus Inc. has appealed the trademark attorney's final refusal to register the mark "CONTENT ALARM" for "computer software that uses linguistic analysis to monitor the transmission of sensitive digital content and provides instant visibility into sensitive information in outgoing network traffic" The examining attorney refused registration on the Principal Register pursuant to Trademark Act Section 2(e)(1), 15 U.S.C. Section 1052(e), because applicant's mark is merely descriptive of the goods. It is respectfully requested that this refusal be affirmed.

FACTS

On July 28, 2003, the applicant filed a Section 1(a) Use-based application for the proposed mark "CONTENT ALARM." The examining attorney issued a first action on February 27, 2004, refusing registration based on Trademark Action Section 2(e)(1). The applicant presented arguments directed at overcoming the descriptiveness refusal in its response filed on August 27, 2004. The examiner was not persuaded by applicant's arguments and issued a final descriptiveness refusal on October 6, 2004. The applicant appealed this refusal and filed its brief on March 8, 2005.

ISSUE

The only issue on appeal is whether the proposed mark "CONTENT ALARM" is merely descriptive of the applicant's goods, namely "computer software that uses linguistic analysis to monitor the transmission of sensitive digital content and provides instant visibility into sensitive information in outgoing network traffic."

ARGUMENT

I. The Mark "Content Alarm" Merely Describes Applicant's Goods.

As the examiner will demonstrate, the applicant's goods comprise software programs used to monitor content on a computer network and warn users of threats regarding access to, and the flow of, that content. The proposed mark "Content Alarm" aptly describes such goods.

The determination of whether a mark is merely descriptive is considered in relation to the identified goods and/or services, not in the abstract. *In re Polo International Inc.*, 51 USPQ2d 1061 (TTAB 1999) (Board found that DOC in DOC-CONTROL would be understood to refer to the "documents" managed by applicant's software, not "doctor" as shown in dictionary definition); *In re Digital Research Inc.*, 4 USPQ2d 1242 (TTAB 1987) (CONCURRENT PC-DOS found merely descriptive of "computer programs recorded on disk;" it is unnecessary that programs actually run "concurrently," as long as relevant trade clearly uses the denomination "concurrent" as a descriptor of this particular type of operating system); *In re Venture Lending Associates*, 226 USPQ 285 (TTAB 1985); *In re American Greetings Corp.*, 226 USPQ 365, 366 (TTAB 1985)

("Whether consumers could guess what the product is from consideration of the mark alone is not the test"); TMEP §1209.01(b).

Moreover, it has long been held that terms that identify the function or purpose of a product or service may be merely descriptive or generic under 15 U.S.C. §1051(e)(1). *In re Gould Paper Corp.*, 834 F.2d 1017, 5 USPQ2d 1110 (Fed. Cir. 1987) (SCREENWIPE held generic for an anti-static cloth used for cleaning computer and television screens); *In re Central Sprinkler Co.,* 49 USPQ2d 1194 (TTAB 1998) (ATTIC generic for sprinklers installed primarily in attics); *In re Reckitt & Colman, North America Inc.*, 18 USPQ2d 1389 (TTAB 1991) (PERMA PRESS generic for soil and stain removers for use on permanent press products); *In re Wallyball, Inc.*, 222 USPQ 87 (TTAB 1984) (WALLYBALL held descriptive of sports clothing and game equipment); *In re National Presto Industries, Inc.,* 197 USPQ 188 (TTAB 1977) (BURGER held merely descriptive of cooking utensils); *In re Orleans Wines, Ltd.*, 196 USPQ 516 (TTAB 1977) (BREADSPRED held merely descriptive of jams and jellies).

Here, the applicant's mark is comprised of two elements, "CONTENT" and "ALARM." The first term is defined as "the subject matter of a written work, such as a book or magazine" or "the substantive or meaningful part." The American Heritage Dictionary of the English Language, *(*3rd ed. Houghton Mifflin Co. 1992). In the context of computer networks and network security, the term is understood to refer to specific user-defined and user-created content resident on the network. This conclusion is supported in the evidence of record. To wit:

> • Privately funded Tablus is tackling the prickly problem of keeping sensitive corporate data from flying out via a network. The Tablus product, an appliance called Content Alarm, monitors outbound network traffic for sensitive **content**, says Jim Nisbet, founder and CEO. "We have to make an analysis quickly when it's a question of proprietary source code or human resources document, for example," Nisbet says.

> The Tablus Content Alarm, which starts at $29,000, works by having agent software on servers where there's sensitive data subject to restricted access. It tracks changes to that **content**, and Content Alarm recognizes when portions of it might be sent out of the network. Ellen Messmer, RSA Conference is a coming-out party for trio of start-ups, Network World, (Feb. 24, 2004), at 20 (emphasis added).
>
> • The **content** security device as been configured to watch for source code contained in the company's version control system from Perforce Software, The hardware also looks for particular financial reports and executive documents stored on a Windows 2003 server…. Choosing the data to protect on the development side was straightforward, since it included all of the company's source and application code. Determining which business documents to protect took more time because it required input from other departments. Antone Gonsalves, Not Just a Game, Compliance Pipeline, (July 21, 2004) at http://www.informationweek.compliancepipeline.com/ showArticle.jhtml?articledId=22103856&printableArticle=true.(emphasis added).
>
> • **Content** Filtering is an automated service residing on a firewall or proxy server that denies your users access to obscene, objectionable or otherwise unallowed **content**. This service is subscription-based as it relies on updates from **content** filtering services. Network Security Solutions at http://www.dnetit.com/security.asp (emphasis added).
>
> • Leakage of a movie ending, a song or even a promotional image before the intended public release date can compromise revenues and marketing launch plans. To keep sensitive media **content** confidential, entertainment companies need a system to monitor their online channels for leakage. Industry Solutions, Media, at http://www.vontu.com/solutions/industrysol.html?src.overture (emphasis added).

Other similarly descriptive usage is found in the extract from the WebmasterWorld.com forum at http://webmasterworld.com/forum17/1587.htm which includes the following discussion:

> "Is there a way to submit non-commercial **content** to Zeal?" I had an editor confirm that community members are blocked from submitting/adding pages from this site to the directory….
>
> "You can't copy the **content** out and into another domain without triggering googles [sic] duplicate content alarms."
>
> It's a page with no commercial **content** on it, simply reference material related to the topic of the site….

The applicant argues in its brief that "content" fails to identify the software "with any one degree of particularity." The examiner disagrees.

The applicant's own website describes the various types of content its goods monitor and protect and lists source code, intellectual property, and customer information as examples. *See* http://www.tablus.com/page.php?id=49. Moreover, the applicant's website touts the software's ability to monitor "content," regardless of composition.

> Tablus Content Alarm provides enterprises visibility into the transmission of sensitive information. It ships as an appliance and can be installed in minutes. It applies fast linguistic analysis to detect the transmission of sensitive **content** or fragments of sensitive **content**. The appliance is armed by letting it examine files that are sensitive. It then derives signatures and vectors that enable it to identify sensitive **content** or fragments of sensitive **content** in network traffic. The **content** to be protected is not stored on the appliance and cannot be recreated from the information that is stored on the appliance. Currently it can detect policy violations in **content** transmitted through FTP, SMTP, HTTP, POP, or IMAP. *See* Product Overview at http://www.tablus.com/products.htm. (emphasis added).

Finally, the applicant itself uses the term "CONTENT" descriptively in its identification of goods, where it describes its goods as "computer software that uses linguistic analysis to monitor the transmission of sensitive digital content."

Therefore, while the definition of "content" may be broad, it cannot be said to be vague or indefinite. As the evidence from applicant's website shows, the term is descriptive when used to refer to material stored on a computer network.

Perhaps in response to the clearly descriptive usage of CONTENT, the applicant focuses the heart of its argument on the descriptiveness of ALARM. Here again, its position is unsupported by the evidence in the record.

"ALARM" is defined as both "a warning of existing or approaching danger," or "an electrical, electronic, or mechanical device that serves to warn of danger by means of a sound or signal." The American Heritage Dictionary of the English Language, (3rd ed. Houghton Mifflin Co. 1992).

The applicant relies heavily on the latter definition. However, the former is equally appropriate. By definition, an "alarm" need not comprise a buzzer, claxon or other audible signal. All that the definition requires is a *warning* of existing or approaching danger.

Applicant notes in its brief "the software is monitoring software that provides notice to the user of the transfer of sensitive corporate data." Appl. Brief at 3. However, the software is far more active than the "video camera monitoring an area for activity" to which the applicant draws a comparison. Id. at 3.

As the applicant's website notes: "Content Alarm can monitor all sensitive information going to the outsourcing provider's network. Another Content Alarm installed at the perimeter of the provider's network alerts the security office immediately if any proprietary data leaves the partner's network." *See* http://www.tablus.com/page.php?id=39.

This "alerting" function is also mentioned in the July 12, 2004 Network World Fusion article, where the software's ability to "scan data as it moves across corporate networks and [ ] trigger alarms if unauthorized files and other digital resources are moved out of the network" is touted. Tim Greene, Tablus boosts capacity of content protection, Network World, (July 12, 2004) at http://www.nwfusion.com/news/2004/071204tablus.html.

Additionally, the section of the applicant's website titled "How It Works" is particularly instructive. Here, the applicant summarizes the content security process utilizing its goods.

> **Install** Content Alarm at a network boundary to monitor outgoing traffic. The boundary may be the company network connection to the Internet or a connection to a subdivision of a company's networks, depending on content security requirements.
>
> **Identify** the sensitive content to protect. Content Alarm provides a number of mechanisms to maintain content classification as the protect content is modified or updated. Patent-pending technology infers content sensitivity by leveraging existing Access Control Lists (ACLs) assigning content classification based on access controls.
>
> **Define** the policies for auditing transmissions. For example, auditing all outgoing network transactions (email, FTP, etc.) that contain sensitive content, or auditing all email sent to a known competitor. Certain transactions, such as a CEO's email, can be exempted from audits.
>
> **Examine** the Content Alarm audit log for policy violations. Only those transmissions that violate explicitly defined policies are audited, leaving only relevant information in the audit log. Content Alarm notifies a content auditor quickly when violations occur. The auditor is then able to see the transmission in detail and determine if it truly reflects a violation of content policies. *See* http://www.tablus.com.page.php?id=49 (emphasis added).

Finally, as noted under the product features, the auditing function of the software features "email, syslog or SNMP notification." This "supports administrator's preferred notification." *See* http://www.tablus.com/page.php?id=49.

Here, unlike the passive video camera analogy raised by applicant, the applicant's software is both assertive and active. As the evidence shows, the applcant's software proactively functions to notify the auditor of a potential violation, thereby providing clear warning to the auditor that sensitive content may have been transmitted from the network. While the duty to respond to that transmission may rest with the auditor, the fact remains that the software actively provides warnings of potential violations. In so doing, the software meets the definition of an "alarm." As such, the applicant's assertion that the goods are "monitoring software, and not alarm software" falls flat.

The applicant maintains that the examiner has misapplied the definition of "alarm." However, it must be noted that the definition proffered by applicant is unduly narrow and ignores completely the more expansive interpretation of an alarm as "a warning of existing or approaching danger." Here, there is no question that the applicant's goods provide a warning of an existing danger, namely that of unauthorized data transmissions.

Furthermore, the goods need not *prevent* data *leaving* the network for the term "ALARM" to be descriptive. The applicant posits that "alarm" would be descriptive if the software prevented data transmission. This strains the American Heritage definition as no such prophylactic function is contemplated under the plain language of the definition.

Moreover, such an interpretation is at odds with the common usage of the term "alarm." Much as "alarm" is considered descriptive when used in "fire alarm" and "burglar alarm" for goods that merely warn of – and do not prevent – fire and burglars, "alarm" in the proposed mark is descriptive for goods that merely warn of threats to network content. Under applicant's interpretation, the term "burglar alarm" would only be descriptive of goods that fail to prevent an intruder's *exit* from the premises. Of course, a common sense interpretation of "alarm" recognizes that a "burglar alarm" is an alarm that warns of a burglar's entry. All that is required under the definition is that the goods provide warning of existing or approaching danger to be aptly described as an alarm.

Finally, the examiner submits that the combination of these two descriptive terms fails to form a new or novel commercial impression. The Board has held that a mark combining descriptive terms is generally not registrable unless the composite creates a unitary mark with a unique, non-descriptive meaning or commercial impression. *In re Tower Tech, Inc.*, 64 USPQ2d 1314 (TTAB 2002) (SMARTTOWER merely descriptive of "commercial and industrial cooling towers and accessories therefor, sold as a unit"); *In re Sun Microsystems Inc.*, 59 USPQ2d 1084 (TTAB 2001) (AGENTBEANS held merely descriptive of "computer software for use in the development and deployment of application programs on a global computer network"); *In re Shiva Corp.*, 48 USPQ2d 1957 (TTAB 1998) (TARIFF MANAGEMENT held merely descriptive for "computer hardware and computer programs to control, reduce and render more efficient wide area network (WAN) usage and printed user manuals sold therewith"); *In re Putnam Publishing Co.*, 39 USPQ2d 2021 (TTAB 1996) (FOOD & BEVERAGE ON-LINE merely descriptive of "a news and information service updated daily for the food processing industry, contained in a database"); *In re Copytele, Inc.*, 31 USPQ2d 1540 (TTAB 1994) (SCREEN FAX PHONE merely descriptive of "facsimile terminals employing electrophoretic displays"); *In re Digital Research Inc.*, 4 USPQ2d 1242 (TTAB 1987) (CONCURRENT DOS and CONCURRENT PC-DOS held merely descriptive of "computer programs recorded on disk").

Here, no new or additional commercial meaning or incongruity is created from the use of the two descriptive terms together. Moreover, the record contains numerous examples where third parties use the terms together in a descriptive manner. The following are worthy of note:

> • Please contact Network Performance Services for additional monitors and to learn about advanced web site monitoring options, such as response time alarms and valid page **content alarms**. *See* http://www.npservices.com/monitor.html(emphasis added).

- **Content Alarm** Software: Vontu Project. Acting as the security checkpoint at every exit on the corporate network, Vontu Project monitors e-mail, web posts, instant messages, FTP and other data for sensitive information. *See* http://search.yahoo.com/search?p=2content+alarms2+ei=UTF-8&fl=0&pstart=1 &fr=FP-tab-web-t&b=21.

- "Wilcox wrote: Looks like all those nasty words "terrorism, "militia" "killing" and of course "blacklist" have tripped someone's **content alarm**;" and "While I know Tangency or even Open would trip my company's web **content alarm**, I generally don't expect this in a review." *See* http://www.google.com/search?q=+2 content+alarm2+-tablus&hl=en&lr=&as_qdr=all&start=10&sa=N.

Based on the evidence above, the public is likely to view the mark in its entirety as descriptive. Furthermore, as noted previously, the examiner believes that amendment to place the mark on the Supplemental Register is appropriate.

CONCLUSION

Therefore, based on the evidence of record, the proposed mark serves merely to describe applicant's goods. Accordingly, the examining attorney requests that the Board affirm the refusal to register the proposed mark on the Principal Register under Section 2(e)(1) of the Trademark Act.

Respectfully submitted,

John T. Lincoski /JTL/
Trademark Attorney
Law Office 113
(571)272-9436

ODETTE BONNET
Managing Attorney
Law Office - 113